WHAT IS CLAIMED IS:

1. A method for distributing information which includes a signature, the method comprising steps of:

generating the signature over first information and second information;

sending the first information over a network;

sending the second information over the network separately from the step of sending the first information; and

sending the signature over the network separately from at least one of the first information and the second information.

2. The method for distributing information of claim 1, wherein the first information comprises an authorization data structure and the second information comprises a software object.

3. The method for distributing information of claim 1, further comprising a step of appending the signature to the first information.

4. The method for distributing information of claim 1, determining which resources a software object in the second information is entitled to interact with.

5. The method for distributing information of claim 1, wherein the step of sending second information comprises a step of waiting a predetermined time period after the step of sending the first information before sending the second information.

6. The method for distributing information of claim 1, wherein the first information includes authorization information for an associated software object.

7. The method for distributing information of claim 1, wherein:

the step of sending the first information comprises transmitting the first information over a first transmission pathway,

the step of sending the second information comprises transmitting the second information over a second transmission pathway different from the first transmission pathway, and

the step of sending the signature comprises transmitting the signature over a third transmission pathway different from at least one of the first and second transmission pathways.

8. A method for detecting modification of information, the method comprising steps of:

receiving first information from a network;

receiving second information from the network separately from the step of receiving the first information;

receiving a signature separately from the network from at least one of the first and second information; and

authenticating the signature over the first and second information.

9. The method for detecting modification of information of claim 8, wherein the first information comprises an authorization data structure and the second information comprises a software object.

10. The method for detecting modification of information of claim 8, wherein:

the step of receiving first information comprises receiving the first information from a first transmission pathway,

the step of receiving second information comprises receiving the second information from a second transmission pathway different from the first transmission pathway, and

the step of receiving a signature comprises receiving the signature from a third transmission pathway different from at least one of the first and second transmission pathways.

11. The method for detecting modification of information of claim 8, further comprising a steps of:

correlating the first information to the second information; and

correlating the signature to the first information and second information.

12. The method for detecting modification of information of claim 8, further comprising a step of determining a lifetime for which the second information is usable.

13. The method for detecting modification of information of claim 8, further comprising a step of checking the first information for an authorization corresponding to the second information.

14. A conditional access system for detecting modification of information, comprising:

an information object;

authorization information, wherein a signature is generated over the information object and the authorization information.

15. The conditional access system of claim 14, further comprising an authorization message which includes the authorization information and the signature.

16. The conditional access system of claim 15, wherein the authorization message includes a plurality of signatures.

17. The conditional access system of claim 16, wherein each of the plurality of signatures uses a different signing algorithm.

18. The conditional access system of claim 14, wherein the authorization information includes authorization tiers which pre-authorize a plurality of information objects.

19. The conditional access system of claim 14, wherein the information object is sent separately over a network from the authorization information.

20. The conditional access system of claim 14, wherein:

the information object uses a first transmission pathway to a set top box,

the authorization information uses a second transmission pathway to the set top box that is different from the first transmission pathway, and

the signature uses a third transmission pathway to the set top box that is different from at least one of the first and second transmission pathways.